UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION AT DAYTON

United States of America,

Plaintiff,

Case No. 3:17-cr-156

v.

Judge Thomas M. Rose

Kyle Bateman,

Defendant.

DECISION AND ENTRY OVERRULING DEFENDANT'S MOTION TO SUPPRESS BASED ON UNCONSTITUTIONAL DEPLOYMENT OF GOVERNMENT SPONSORED MALWARE DUBBED THE "NETWORK INVESTIGATIVE TECHNIQUE," ECF 14, DEFENDANT'S MOTION TO SUPPRESS BASED ON A LACK OF KNOWING WAIVER OF DEFENDANT'S PRIVILEGE AGAINST SELF-INCRIMINATION AND DEFECTIVE *MIRANDA* WARNING, ECF 15, AND DEFENDANT'S MOTION TO SUPPRESS EVIDENCE AND MOTION FOR *FRANKS* HEARING. ECF 17

Pending before the Court are Defendant's Motion to Suppress Based on Unconstitutional Deployment of Government Sponsored Malware Dubbed the "Network Investigative Technique," ECF 14, Defendant's Motion to Suppress Based on a Lack of Knowing Waiver of Defendant's Privilege against Self Incrimination and Defective *Miranda* Warning, ECF 15, and Defendant's Motion to Suppress Evidence and Motion for *Franks* Hearing. ECF 17.

I. Background

The seminal events of this case are well-established, and have been previously considered by the Court:

> Between September of 2014 and February 3, 2015, Special Agents employed by the Maryland Federal Bureau of Investigation acquired control of a website that they believed contained illicit material that included child pornography. The Government began to operate the website from their facility located in Virginia, which continued to distribute pornography and bulletin boards which posted messages, images, videos and other miscellaneous material.
>
> On or about February 20, 2015, Special Agent Macfarlane applied for a search warrant permitting the use of Network Investigative Techniques ("NIT"). The government's purpose of the NIT was to identify any potential users that accessed the website between February 20, 2015 and March 4, 2015. The NIT would deploy from the government-controlled network to the accessing computer and search that computer in order to obtain its IP address, user ID, password and host name. Then, the NIT would communicate the information found in its search back to the government-operated server. Once the government had the computer's identification information, the government would obtain a warrant to search the person's computer, home, and other electronic devices associated with the IP address.

United States v. Jones, 230 F. Supp. 3d 819, 821-22 (S.D. Ohio 2017).

On August 19, 2015, law enforcement officials executed a search warrant at Defendant Kyle Bateman's residence located at 1017 Beryl Trail, Washington Township, Ohio. (3:15-mj-271). In conjunction with the execution of this search warrant, FBI agents interviewed Defendant at the FBI's Centerville, Ohio office. This interview was audio and video recorded. At the outset of the interview, Defendant was provided with *Miranda* warnings. Defendant admits, "At 3:09 the agent begins to give Mr. Bateman the *Miranda* warning. Defendant listened to the Miranda warnings…." ECF 15, at PageID 94.

On September 28, 2017, a federal grand jury returned a single-count indictment against Defendant charging him with possession of child pornography in violation 18 U.S.C. § 2252(a)(4)(B). (ECF 3, Indictment).

II. Analysis

In Defendant's Motion to Suppress Based on Unconstitutional Deployment of Government Sponsored Malware Dubbed the "Network Investigative Technique," ECF 14, Defendant urges the Court to find that the NIT conducted a search of Defendant's computer, that its operation was a search and seizure, not a tracking device. Defendant reasons his computer would not—and could not—have been legally contacted by the NIT had the Federal Rule of Criminal Procedure 41[1] been followed because his computer lay outside the statutorily circumscribed reach of the issuing magistrate judge's power. Defendant urges that this requires that the fruits of what it considers a search of his computer to be suppressed.

The Court has previously considered the Network Investigative Technique, (NIT), to be a tracking device. See *United States v. Jones*, 230 F. Supp. 3d 819, 823 (S.D. Ohio 2017)(Rose, J.). The Court has not changed its view. Moreover, even if there is a Rule 41 violation of a constitutional magnitude, the Court would still not suppress because of the *Leon* good faith rule. Thus, Defendant's Motion to Suppress Based on Unconstitutional Deployment of Government Sponsored Malware Dubbed the "Network Investigative Technique," ECF 14, will be denied.

The Court next considers Defendant's Motion to Suppress Based on a Lack of Knowing Waiver of Defendant's Privilege against Self Incrimination and Defective *Miranda* Warning. ECF 15. *Miranda* warnings are required when a "suspect's freedom of action is curtailed to a degree associated with a formal arrest." *Berkemer v. McCarty*, 468 U.S. 420, 440 (1984)). The obligation of law enforcement officers to administer *Miranda* warnings to a suspect arises "where

1 Since modified.

there has been such a restriction on a person's freedom as to render him 'in custody.'" *Oregon v. Mathiason*, 429 U.S. 492, 495 (1977). Here, Defendant was advised of his *Miranda* rights prior to making any statements. ECF 15, at PageID 94. Thus, even if he was under arrest, he is not entitled to suppression. Therefore, Defendant's Motion to Suppress Based on a Lack of Knowing Waiver of Defendant's Privilege against Self Incrimination and Defective *Miranda* Warning, ECF 15, will be denied.

Finally, the Court considers Defendant's Motion to Suppress Evidence and Motion for *Franks* Hearing. ECF 17. In order to obtain a *Franks* hearing, a defendant must make a substantial preliminary showing that (1) the affiant's statement was deliberately false or demonstrated reckless disregard for the truth, *Franks v. Delaware*, 438 U.S. 152, 155-56, 171 (1978), and (2) the challenged statement or omission was essential to the magistrate's finding of probable cause. Id. at 155-56, 171-72. To the extent a defendant relies on "recklessness," the test is a subjective one. *United States v. Cican*, 63 Fed. App'x 832, 835-36 (6th Cir. 2003); *United States v. Colquitt*, 604 Fed. App'x 424, 429-30 (6th Cir. 2015). A law enforcement officer's statement is made with "reckless disregard for the truth" when he or she subjectively "entertains serious doubts as to the truth of his [or her] allegations." *United States v. Cican*, 63 Fed. App'x at 836. "Only after the defendant makes this showing may the court consider the veracity of the statements in the affidavit or the potential effect of any omitted information." *United States v. Archibald*, 685 F.3d 553, 558-59 (6th Cir. 2012). "Without this substantial showing, courts may not make a *Franks* ruling regarding the veracity of statements made in an affidavit." Id. at 559. A defendant seeking a *Franks* hearing "should point out specifically the portion of the warrant affidavit that is claimed to be false." *Franks*, 438 U.S. at 170.

Defendant asserts that Agent MacFarlane gave "a false description of 'Website A's' home

page, which was the single most important piece of the probable cause puzzle", and "false statements about the place to be searched pursuant to the NIT warrant." (ECF 17 at PageID 324). Defendant attempts to characterize the Playpen website as merely a source of innocent child erotica. The descriptions of the threads and images that Defendant viewed on Playpen exceed what one might anticipate containing legal child erotica. Defendant's second premise is a re-packaging of the same argument he asserted in Motion to Suppress Based on Unconstitutional Deployment of Government Sponsored Malware Dubbed the "Network Investigative Technique." ECF 14.

Even had Defendant made a substantial preliminary showing of falsity, he would still not be entitled to a *Franks* hearing. Defendant must also make a substantial preliminary showing that the falsehood was made deliberately or with reckless disregard for the truth. Since this test is a subjective one, Defendant must make a substantial preliminary showing that Agent Macfarlane not only relayed to the Magistrate Judge by way of his affidavit false information, but did so deliberately or with reckless disregard for the truth. No such showing has been made to support such a claim.

Finally, even had Defendant made a substantial preliminary showing of both falsity and deliberateness or recklessness, he still would not be entitled to a *Franks* hearing without also establishing materiality. Defendant does not address the issue of materiality in his motion. Excising what Defendant believes is false from Agent Macfarlane's supporting affidavit still leaves sufficient facts to establish the necessary probable cause to have properly issued the NIT warrant.

For these reasons, Defendant's Motion to Suppress Based on Unconstitutional Deployment of Government Sponsored Malware Dubbed the "Network Investigative Technique," ECF 14,

Defendant's Motion to Suppress Based on a Lack of Knowing Waiver of Defendant's Privilege against Self Incrimination and Defective *Miranda* Warning, ECF 15, and Defendant's Motion to Suppress Evidence and Motion for *Franks* Hearing, ECF 17, are **OVERRULED.**

DONE and **ORDERED** this Monday, April 23, 2018.

s/Thomas M. Rose

THOMAS M. ROSE
UNITED STATES DISTRICT JUDGE